Email Spam Triage Guide

Symptoms of a compromised email account:

- Unable to send emails from the account.
- Unable to receive emails from other accounts.
- Receiving an abnormally large amount of spam emails.
- Receiving “undeliverable” messages from unknown accounts.
- User admitting to clicking on phishing link.
- Any other unusual activity within email account.

Steps to fix compromised account:

1. Change your network password on my.sc.edu. If the password is not updated, any steps to remedy the situation will simply be reverted since the hacker still has access to the account.
Change the password to something that is not similar to or the same as any password they have previously used. If the password is similar to the password the hacker is in possession of, it would be easy to hack the account again.
2. With the new network password, log into the student email account, click the gear icon in the top right hand corner, and click options.

3. Click “Forwarding” in the left hand pane. If there is an unrecognized email listed in the forwarding section, click “Discard”.

   ![Options menu](image)

   ![Forwarding settings](image)
4. Click “Connected Accounts” in the left hand pane. Delete any unknown accounts by clicking on the account listed and then clicking the trash can icon.

5. Click “Inbox Rules” in the left hand pane. Delete any unknown rules by clicking on the rule and then clicking the trash can icon.
6. Test the email by sending emails back and forth with another account. If everything is working, then the issue is resolved.

7. If the account is still not able to send or receive emails, please contact the UTS Service Desk at (803) 777-1800.